

**WHAT IS CLAIMED IS:**

- 1 1. A method of managing customer security features by a  
2 security server, said method comprising:  
3 receiving a request from a requestor;  
4 authenticating the requestor; and  
5 manipulating one or more security features stored in a  
6 data area corresponding to a customer in response  
7 to the request.
- 1 2. The method as described in claim 1 wherein at least  
2 one of the security features is selected from the  
3 group consisting of a photograph of the customer, a  
4 customer signature, a digital signature corresponding  
5 to the customer, a fingerprint, and a description of  
6 the customer.
- 1 3. The method as described in claim 1 further comprising:  
2 receiving one or more new security features from the  
3 customer;  
4 assigning an item identifier to each of the new  
5 security features; and  
6 storing the new security features in the data area  
7 corresponding to the customer.
- 1 4. The method as described in claim 1 further comprising:  
2 receiving an authorization from a customer, the  
3 authorization including a first merchant  
4 identifier;  
5 storing the authorization;  
6 receiving a retrieval request from a merchant, the  
7 retrieval request including a customer identifier

8 corresponding to the customer and a second  
9 merchant identifier corresponding to the  
10 merchant;  
11 validating the merchant request, the validating  
12 including:  
13 retrieving the authorization; and  
14 comparing the first merchant identifier to the  
15 second merchant identifier; and  
16 returning one or more security features corresponding  
17 to the customer in response to the first merchant  
18 identifier matching the second merchant  
19 identifier.

1 5. The method as described in claim 1 further comprising:  
2 receiving an authorization from a customer, the  
3 authorization including a public key  
4 corresponding to the merchant;  
5 storing the authorization and the merchant's public  
6 key;  
7 receiving an encrypted retrieval request from a  
8 merchant, the encrypted retrieval request  
9 encrypted using a private key corresponding to  
10 the merchant's public key;  
11 deciphering the encrypted retrieval request using the  
12 stored public key; and  
13 returning one or more security features corresponding  
14 to the customer in response to the deciphering.

1 6. The method as described in claim 1 further comprising:  
2 receiving an edit request from a customer, the edit  
3 request including a customer identifier and one  
4 or more updated security features, the security

5 features each including an security item  
6 identifier;  
7 locating a stored security feature corresponding to  
8 each of the security item identifiers; and  
9 replacing the stored security features with the  
10 updated security features.

1 7. The method as described in claim 6 further comprising:  
2 verifying the customer, the verifying including:  
3 receiving a secret customer identifier from the  
4 customer; and  
5 comparing the secret customer identifier with a  
6 stored secret customer identifier  
7 corresponding to the customer.

1 8. The method as described in claim 1 wherein the request  
2 includes an encrypted packet that is encrypted using a  
3 private key corresponding to the requestor, the method  
4 further comprising:  
5 locating a stored public key corresponding to the  
6 requestor; and  
7 deciphering the encrypted packet using the stored  
8 public key, the deciphering verifying the  
9 identity of the requestor, wherein the  
10 manipulating is performed in response to the  
11 encrypted packet being successfully deciphered.

1 9. An information handling system comprising:  
2 one or more processors;  
3 a memory accessible by the processors;  
4 a network interface for communicating with other  
5 information handling systems;

one or more nonvolatile storage areas accessible by  
the processors; and  
a security feature management tool to manage customer  
security features, the security feature  
management tool including:  
means for receiving a request from a requestor;  
means for authenticating the requestor;  
means for manipulating one or more security  
features stored in a data area corresponding  
to a customer in response to the request.

10. The information handling system as described in claim  
9 wherein the request includes an encrypted packet  
that is encrypted using a private key corresponding to  
the requestor, the information handling system further  
comprising:  
means for locating a stored public key corresponding  
to the requestor; and  
means for deciphering the encrypted packet using the  
stored public key, the deciphering verifying the  
identity of the requestor, wherein the  
manipulating is performed in response to the  
encrypted packet being successfully deciphered.

11. The information handling system as described in claim  
9 further comprising:  
means for receiving an authorization from a customer,  
the authorization including a first merchant  
identifier;  
means for storing the authorization;  
means for receiving a retrieval request from a  
merchant, the retrieval request including a

21 customer identifier corresponding to the customer  
22 and a second merchant identifier corresponding to  
23 the merchant;  
24 means for validating the merchant request, the  
25 validating including:  
26 retrieving the authorization; and  
27 comparing the first merchant identifier to the  
28 second merchant identifier; and  
29 means for returning one or more security features  
30 corresponding to the customer in response to the  
31 first merchant identifier matching the second  
32 merchant identifier.

1 12. The information handling system as described in claim  
2 9 further comprising:  
3 means for receiving one or more new security features  
4 from the customer;  
5 means for assigning an item identifier to each of the  
6 new security features; and  
7 means for storing the new security features in the  
8 data area corresponding to the customer.

1 13. A computer program product stored on a computer  
2 operable medium for managing customer security  
3 features by a security server, said computer program  
4 product comprising:  
5 means for receiving a request from a requestor;  
6 means for authenticating the requestor; and  
7 means for manipulating one or more security features  
8 stored in a data area corresponding to a customer  
9 in response to the request.

1 14. The computer program product as described in claim 13  
2 wherein at least one of the security features is  
3 selected from the group consisting of a photograph of  
4 the customer, a customer signature, a digital  
5 signature corresponding to the customer, a  
6 fingerprint, and a description of the customer.

1 15. The computer program product as described in claim 13  
2 further comprising:  
3 means for receiving one or more new security features  
4 from the customer;  
5 means for assigning an item identifier to each of the  
6 new security features; and  
7 means for storing the new security features in the  
8 data area corresponding to the customer.

1 16. The computer program product as described in claim 13  
2 further comprising:  
3 means for receiving an authorization from a customer,  
4 the authorization including a first merchant  
5 identifier;  
6 means for storing the authorization;  
7 means for receiving a retrieval request from a  
8 merchant, the retrieval request including a  
9 customer identifier corresponding to the customer  
10 and a second merchant identifier corresponding to  
11 the merchant;  
12 means for validating the merchant request, the  
13 validating including:  
14 retrieving the authorization; and  
15 comparing the first merchant identifier to the  
16 second merchant identifier; and

17 means for returning one or more security features  
18 corresponding to the customer in response to the  
19 first merchant identifier matching the second  
20 merchant identifier.

1 17. The computer program product as described in claim 13  
2 further comprising:  
3 means for receiving an authorization from a customer,  
4 the authorization including a public key  
5 corresponding to the merchant;  
6 means for storing the authorization and the merchant's  
7 public key;  
8 means for receiving an encrypted retrieval request  
9 from a merchant, the encrypted retrieval request  
10 encrypted using a private key corresponding to  
11 the merchant's public key;  
12 means for deciphering the encrypted retrieval request  
13 using the stored public key; and  
14 means for returning one or more security features  
15 corresponding to the customer in response to the  
16 deciphering.

1 18. The computer program product as described in claim 13  
2 further comprising:  
3 means for receiving an edit request from a customer,  
4 the edit request including a customer identifier  
5 and one or more updated security features, the  
6 security features each including an security item  
7 identifier;  
8 means for locating a stored security feature  
9 corresponding to each of the security item  
10 identifiers; and

11 means for replacing the stored security features with  
12 the updated security features.

1 19. The computer program product as described in claim 18  
2 further comprising:  
3 means for verifying the customer, the verifying  
4 including:  
5 means for receiving a secret customer identifier  
6 from the customer; and  
7 means for comparing the secret customer  
8 identifier with a stored secret customer  
9 identifier corresponding to the customer.

1 20. The computer program product as described in claim 13  
2 wherein the request includes an encrypted packet that  
3 is encrypted using a private key corresponding to the  
4 requestor, the computer program product further  
5 comprising:  
6 means for locating a stored public key corresponding  
7 to the requestor; and  
8 means for deciphering the encrypted packet using the  
9 stored public key, the deciphering verifying the  
10 identity of the requestor, wherein the  
11 manipulating is performed in response to the  
12 encrypted packet being successfully deciphered.